PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00 — A2

(11) International Publication Number: **WO 00/00882**

(43) International Publication Date: 6 January 2000 (06.01.00)

(21) International Application Number: PCT/US99/14554

(22) International Filing Date: 25 June 1999 (25.06.99)

(30) Priority Data:
60/090,822 27 June 1998 (27.06.98) US

(71) Applicant: LCI/SMARTPEN, N.V. [US/US]; 952 Beacon Street, Newton, MA 02159 (US).

(72) Inventor: DE SCHRIJVER, Stefaan, A.; 952 Beacon Street, Newton, MA 02159 (US).

(74) Agents: KELLY, Edward, J. et al.; Foley, Hoag & Eliot, LLP, One Post Office Square, Boston, MA 02109 (US).

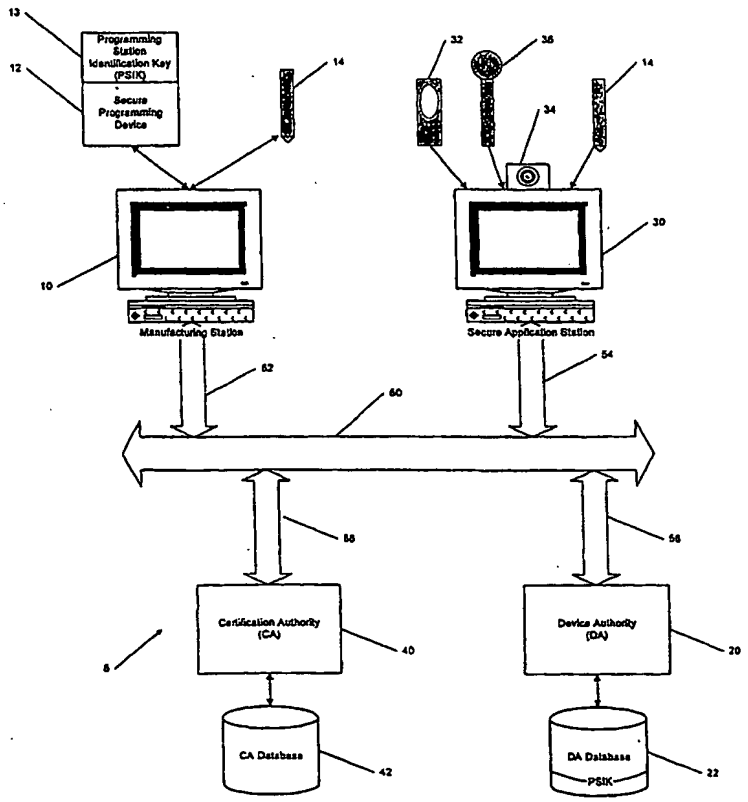
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: APPARATUS AND METHOD FOR END–TO–END AUTHENTICATION USING BIOMETRIC DATA

(57) Abstract

A secure transaction system and a secure method for authenticating a user based on biometric data of the user includes a biometric analyzer device that is assembled in a secure environment and has a secure device identifier and encryption key. First authentication means receive the biometric data and authenticate the biometric data of the user based on biometric reference data from the user, while second authentication means authenticate an authorized use of the biometric analyzer device based on at least the secure device identifier. The secure transaction system authenticates the user only if both the first and second authentication means authenticate the biometric data and the authorized use of the biometric input device, respectively.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

APPARATUS AND METHOD FOR END-TO-END AUTHENTICATION USING BIOMETRIC DATA

Cross-Reference to Related Applications

The present application claims the benefit of the filing date of the provisional application Serial No. 60/090,822, which has a filing date of June 26, 1998.

Background of The Invention

1. Field of the invention

The invention relates to the field of authentication, fraud detection and prevention, security and cryptography. More particularly, the invention relates to the authentication of biometric data.

2. Description of Related Art

With the emergence of Electronic Commerce, various processes have been devised for authenticating users and ensuring the privacy of electronic data transmitted and received by the users. Governments in many countries designate and accredit appropriate organizations to perform specific roles for secure data transmission, including digital signature.

Electronic commerce may require several distinct security elements: Authentication, Secure Communications, Trusted Server Environments, Electronic Contracts, Protection of Intellectual Property, Digital Payment mechanisms, and Corporate Information Security (Data, Processes, Access Control)

Technologies commonly employed to detect and react to breach of confidentiality, fraud and piracy include cryptography, which provides the mathematical framework for secure document transmission and authentication; key registration and certification for enhancing proof of authenticity; tokens for providing safety of physical

information; biometric analysis for linking verifiable physical user attributes (biometric properties) with the authentication process; and tamper-resistant devices for safe storage and processing of intrinsic physical information.

By way of background, cryptographic methods can be divided into symmetric and asymmetric methods, depending on the keys used to encrypt and decrypt messages. Symmetric ("Private Key") cryptography uses the same key both for encrypting and decrypting a message. A message is understood to represent an arbitrary data string which may be represented by binary, octal, hexadecimal number, as is known in the art. Since the same key is used for both encryption and decryption, the key must always be kept secret and delivered to another party in a secure fashion. Anyone in possession of the symmetric decryption key can also encrypt, making it impossible to authenticate the originator.

Asymmetric Key ("Public/Private Key pair") cryptography is based on two keys which are mathematically related to one another to form a complement. For example, one of the keys can be used to encrypt a data string, while the other key can be used to decrypt the data string. One key, called the Private Key, is kept secret. The other key, called the Public Key, is not secret and may be distributed without jeopardizing security. Public-Key cryptography is well known in the art.

Asymmetric Key arrangements can be used in two ways: for secure encryption of data strings, or to authenticate the originator of the data. However, the same key pair cannot be used simultaneously to encrypt the data strings and for authenticating the originator.

Another useful concept in cryptography are one-way functions, noticeably one-way hash functions. A hash function is a function that takes an input string and converts it to a fixed-size, often smaller output string. Since hash functions are typically many to one, they cannot be used to determine with absolute certainty if two input strings are equal; however, if two input strings hash to the same value, they two input strings are identical with an overwhelming degree of certainty. In other words, the hash values

cannot be decrypted. To enhance security further, the hashed output string can be encrypted with the recipients public key, which the recipient then decrypts with his private key. One-way functions have to major applications: password protection and message digesting. Examples for password protection using one-way functions can be found on modern computers to verify access authorization. Examples for message are the MD4 and MD5 algorithms, which are known in the art.

Another useful concept is that of a Digital Signature. To secure a message, one can attach to it a Digital Signature. A person creates a message as described above. The sender of an original message produces a one-way hash of the message, i.e., the message digest, and encrypts the hash with the sender's Private Key. The sender then attaches the message digest and the Private Key to the original message. This attachment is called a Digital Signature. The sender sends to the recipient the original message and the message digest, as well as information which allows the recipient to compute the sender's Public Key. Digital Signatures can authenticate that the Private Key of the sender was indeed used with the original document and verify that the original document has not been altered.

Without additional safeguarding, however, the recipient has no way, based on the transmitted information alone, to verify the true identity of the sender. In other words, the recipient cannot verify that the sender and the person from which the recipient expects the message, are identical.

To remedy these shortcomings, the ISO authentication framework, also known as X.509 protocol, was established. The framework is certificate-based. A trusted certification authority (CA) assigns a unique name to each user and issues a certification certificate containing the name and the user's public key. The CA signs all certification certificates with a secret key. Certification certificates may have a specified validity period. However, unless the user is personally known to the CA, the CA is still not able to guarantee that the user actually is the physical person associated with the user name. Such guarantee is provided by a Registration or Device Authority (DA).

The DA verifies the identity of the user and issues a Private Key/Public Key arrangement. The person's Private Key is typically a password which the person has to remember, and/or a token that contains the Private Key. The DA encrypts the information about the person, including the person's public key, using the DA's Private Key, digitally signs the encrypted information and makes the information available to CA's for storage on a key server. The signed encrypted information is called a Registration Certificate.

The CA distributes the Registration Certificate on a server, and certifies them as authentic based on the DA's public key which the CA has in its possession. The CA's public keys are incorporated into most browsers. A person can verify another person by using the certification authority's public key. In this way the requesting person can know that the Certificate is authentic. Certificates are not limited to a single sender and a single recipient. If several people are involved in a transaction, a Certificate must be certified for each party. The plurality of Certificates must be attached to the message digest corresponding with the transaction. As mentioned above, all Certificates are deemed authentic.

However, the Certification Authority may issue an authentic Certificate based on the correct Private Key or Token of the user, although the user was not authenticated. For example, secure Private Keys may have a considerable number of characters, making them difficult to remember. An authenticated user may therefore be tempted to record the password either on paper or in a computer file as plain text, which may then be misappropriated by a potential perpetrator. Passwords may also be recorded when entered into a security station and fraudulently replayed at a later time. Tokens containing the Private Key, on the other hand, may be misappropriated or stolen.

It is therefore desirable to uniquely establish a secure link between a person and the Private Key being used by that person in such a way that the Private Key can only be used by that person. It is further desirable to establish a Private Key for a person which is unique and does not have to be recorded or memorized

Summary of the Invention

In general, the present invention combines biometric authentication, electronic signatures, digital signatures, device identification, and an apparatus for secure manufacturing with symmetric and asymmetric cryptography to enable end-to-end security of electronic transactions.

According to one aspect of the invention, a secure transaction system for authenticating a user based on the user's biometric data includes a biometric analyzer device that receives the biometric data of the user and has a secure device identifier. The secure transaction system authenticates the user only if both a first authentication means, which receives the biometric data, authenticates the biometric data of the user based on biometric reference data of the user, and a second authentication means authenticates an authorized use of the biometric analyzer device based on at least the secure device identifier.

According to another aspect of the invention, a method for authenticating biometric data of a user includes providing a biometric analyzer device with a secure device identifier, acquiring with the biometric analyzer device biometric data of the user, and generating a sequentially increasing session ID for successive acquisitions of the biometric data. The method further includes authenticating the biometric analyzer device based on at least the secure device identifier, and authenticating the biometric analyzer data based on at least the session ID and a comparison between the acquired biometric analyzer data and reference biometric data for the user. The biometric data are authenticated only if both the biometric analyzer device and the biometric analyzer data are authentic.

According to yet another aspect of the invention, a method for providing end-to-end security in a transaction using biometric data includes programming a biometric analyzer device with a secure device identifier, assigning a secure device key to the biometric analyzer device, and acquiring the biometric data with the biometric analyzer device, wherein the biometric analyzer device generates a respective sequentially increasing session ID for successive recordings of the biometric data. The method

further includes authenticating the biometric data based on at least the secure device identifier, the device key and the session ID, and on a comparison of a representation of the acquired biometric data with a representation of reference biometric data recorded with the same biometric analyzer device.

Embodiments of the invention may include one or more of the following features. The biometric analyzer device may generate a unique session ID for each user session, wherein the unique session ID may be sequentially increasing from one session to the next. The user is authenticated only if the session ID of the current session is greater than the session ID of the previous session for the respective biometric analyzer device. The biometric analyzer device may include a unique biometric analyzer key which is issued by a trusted device authority and stored tamper-proof in the biometric analyzer device. The biometric analyzer device may be programmed by a secure programming device having a secure programming station identification key which is known to the trusted device authority. The secure programming device may include a programming station identification key which may be a symmetric key provided by a trusted device authority. As a further security measure, the biometric analyzer device may also include a biometric analyzer key, wherein authentication of the biometric analyzer device depends on a comparison of the biometric analyzer with a reference key maintained by a trusted device authority. The biometric data may be in the form of a message digest or hash.

Further features and advantages of the present invention will be apparent from the following description of preferred embodiments and from the claims.

Brief description of the Drawings

FIG. 1 is a schematic block diagram of a system for end-to-end authentication of biometric data according to the invention,

FIG. 2 shows the interactions between various devices and the Device Authority during manufacture and initialization of the Biometric Analyzer Device,

FIG. 3 shows the interactions between the secure application station and the registration and certification authorities during authentication of biometric data,

FIG. 4 is a flow diagram of the manufacturing process of a Biometric Analyzer Device according to the invention, and

FIG. 5 is a flow diagram of the authentication process according to the invention.

Description of Preferred Embodiments

Referring now to FIG. 1, a secure manufacturing and authentication system 5 for end-to-end authentication of biometric data includes a manufacturing station 10 at which an exemplary Biometric Analyzer Device 14, shown here in form of a pen 14, for entering a user's signature, is assembled. The pen 14 may be, for example, a LCI-SMARTpen™ available in the USA from LCI-SMARTpen, Andover, MA. The LCI-SMARTpen™ includes an advanced wireless computer system which is miniaturized to have the same footprint and performance as a pen.

Instead of or in addition to the pen 14, the Biometric Analyzer Device may include other biometric input devices, such as a fingerprint reader 32, a voice recognition device 36, an optical face or iris scanner 34, and the like. Although the invention will be described hereinafter with respect to the pen input device 14, it will be understood by those skilled in the art that the apparatus and method of the invention are applicable to other biometric input devices as well. The electronic circuit of the Biometric Analyzer Device 14 includes electronic chips for data acquisition, data processing and data output. At least one of the chips typically includes a programmable or re-programmable chip ID provided by the chip manufacturer. This chip ID is unique but not secure, because it is known by the chip manufacturer. To improve the security of the stored identification numbers, the manufacturing station 10 includes a Secure Programming Device 12 which is tamper-resistant and contains a unique Private Key, called a Programming Station Identification Key (PSIK) 13. The Secure Programming Device 12 with the PSIK 13 is installed by a trusted third party, such as a Device Authority (DA) 20. Details of the interactions between the Secure Programming Device

12, the Biometric Analyzer Device 14 and the DA 20 will be discussed in more detail below. The manufacturing station 10 may interact with the DA 20 via data lines 50, 52 and 56, which may be secure or open communication channels, in a manner known in the art.

The electronics in the Biometric Analyzer Device 14 are physically protected by conventional tamper-resistant electronic packaging. The unique but public ID number of the programmed chip in the Biometric Analyzer Device 14 is stored in the device 14 as a Chip ID 15. The Biometric Analyzer Public Key, which will be discussed later, also remains with the Biometric Analyzer Device at all times. These data are unalterable and can be read only inside the Biometric Analyzer Device.

The secure manufacturing and authentication system 5 communicates with a Certification Authority (CA) 40 which has knowledge about the encryption keys used by the DA 20 and is responsible for issuing a certificate once the biometric data have been authenticated. Both the Device Authority 20 and the Certification Authority 40 maintain respective databases 22, 42 which store attributes of the Biometric Analyzer Devices 14 required for verification and authentication of the biometric data. For example, the PSIK is securely stored in the DA database 22.

Another part of the secure manufacturing and authentication system 5 for providing end-to-end security is a secure application station 30 to which the Biometric Analyzer Device 14 can be connected. For the purpose of authentication, the secure application station 30 interacts with the DA 20 and the CA 40. Details of this interaction will be discussed in detail below.

Referring now to FIG. 2, during manufacture of the Biometric Analyzer Device 14, the Secure Programming Device 12 of the manufacturing station 10 sends the chip ID (C-ID) 15 of the Biometric Analyzer Device 14 to a trusted third party, in this case the Device Authority (DA) 20, in the form of a message digest by hashing the chip ID 15 with the Programming Station Identification Key (PSIK) 13, as indicated by arrow 16. The Device Authority 20 recognizes the PSIK and generates a biometric analyzer

public/private key arrangement (BAID). The Device Authority 20 stores the chip ID 15 and the BAID in its database 22 corresponding to the PSIK.

The Device Authority 20 encrypts the BAID using the PSIK and sends the encrypted BAID to the Secure Programming Device 12 corresponding to the PSIK, as indicated by arrow 17. The Secure Programming Device 12 decrypts the received the encrypted BAID and embeds the Biometric Analyzer's private key into the Biometric Analyzer Device 14, as indicated by arrow 18. The BAID public key travels with the Biometric Analyzer Device 14 to the secure application station 30 which will be described in more detail below. In addition, the Device Authority 20 communicates the PSIK also to the Certification Authority 40 via a secure transmission channel (not shown).

Referring now to FIG. 3, the Biometric Analyzer Device 14 of the secure application station 30 acquires biometric user input data. The secure application station 30 generates a biometric message digest (hash) of a transaction including an electronic signature of the Biometric Analyzer Device. The secure application station 30 transmits the hashed and signed transaction data to the Certification Authority 40 as a trusted third party, as indicated by arrow 25. The Certification Authority 40 sends the BAID for verification to the Device Authority 20, as indicated by arrow 27. If the private key and the public key match the PSIK keys stored in the DA database 22, the Device Authority 20 issues a security certificate to the Certification Authority 40, as indicated by arrow 28. The Device Authority 20 may also make an entry into the record in its database 22 corresponding to the PSIK. As mentioned above, the Device Authority 20 communicates the PSIK to the Certification Authority 40 via a secure communication channel. The Certification Authority 40 checks the electronic signature of the Biometric Analyzer Device 14 based on records in its database 42.

One of two situations can occur: If this is the first time the user enters biometric data into the Biometric Analyzer Device 14, a trusted third party has to verify the user's true identity. The trusted third party may be, for example, a bank, a notary and the like, that is in possession of an authenticated private key. The corresponding public key

would be known to the various certification authorities. The trusted third party signs the biometric data or a hash thereof which is considered by the respective certification authority receiving the biometric data as proof that the biometric data are genuine and are associated with the identified user. The respective certification authority stores the user and biometric data attributes in its secure database.

If, on the other hand, the user's biometric data are already referenced in the respective Certification Authority's database, an authentication algorithm of the Certification Authority 40 compares the received biometric data with the referenced biometric data. If these data are in agreement and if a valid security certificate was received from the Device Authority 20, then the Certification Authority 40 issues of an Authentication Certificate, as indicated by arrow 26. Issuance of the certificate may also be recorded in the CA database 42.

Referring now to FIG. 4, a flow diagram depicts the secure generation of device identifiers for the Biometric Analyzer Device 14. The secure generation of device identifiers essentially can be separated into two parts: a process 60 for generating a secure device identifier based on the tamper-resistant Programming Station Identification Key (PSIK) 13, and a process 70 by which the Device Authority 20 that also has possession of the PSIK generates Biometric Analyzer Private/Public key pairs for the device having the respective PSIK. In process 60, a chip manufacturer providing electronic components for the Biometric Analyzer Device loads a unique chip ID into the Biometric Analyzer Device, step 62. The Secure Programming Device reads the chip ID provided by the chip manufacturer, step 64. The chip ID is unique, but not secure, because it is known by the chip manufacturer, as discussed above. Next, the Secure Programming Device generates a sequence number (SN), step 66. The Secure Programming Device then uses its PSIK to encrypt the chip ID and the sequence number, step 68, and sends the encrypted information to the Device Authority (DA), step 69.

In process 70, the Device Authority, upon verification of the PSIK, symmetrically decrypts the encrypted information. The Device Authority generates for

the device associated with the PSIK a Biometric Analyzer Public/Private Key (BAID) arrangement by conventional key generation methods, such as RSA, step 72. The Device Authority stores the chip ID with the Biometric Analyzer Identification Public and Private Keys (BAID) in a secure database, step 74. The database is secured by conventional means known in the art. The Device Authority then encrypts the BAID using the appropriate PSIK, and sends the encrypted BAID to the Secure Programming Device that corresponds with the respective PSIK, step 76.

The Secure Programming Device, upon receipt of the encrypted BAID, decrypts the BAID with its PSIK and embeds the Biometric Analyzer Private Key into the programmable integrated circuit of the Biometric Analyzer Device currently being assembled at the manufacturing station, step 78, using a Write Once Read Many process. Write Once Read Many (WORM) processes are well known in the art. The Biometric Analyzer Device is now ready to record biometric data from a user.

Referring now to FIG. 5, a flow diagram depicts a process 80 for recordation of biometric data and a process 90 for authentication of the biometric data acquired with an authenticated Biometric Analyzer Device. In process 80, the Biometric Analyzer Device 14 records user biometric data, step 82, and generates a sequentially increasing Session-ID, step 84. The recorded biometric data together with the BAID private key and the Session-ID are encrypted with the BAID public key, step 86, before the data leave the Biometric Analyzer Device. The encrypted data are then hashed into a message digest and digitally signed, whereafter the hashed and signed data are securely transmitted to the Certification Authority (CA). The Certification Authority (CA) decrypts the message digest, step 92. The Certification Authority then checks if the session ID is greater than a session ID previously received for the same device, step 94. If the Session ID is greater than the last recorded session ID, the Certification Authority contacts the Device Authority which knows the BAID Public and Private keys for the respective Chip-ID. If the BAID is correct, step 98, the DA issues a security certificate to the Certification Authority, step 100. Upon receipt of the security certificate and after reviewing the biometric data and comparing the biometric data with corresponding reference biometric data contained in the CA database 42, the Certification Authority

issues its own certificate, which may be time and date stamped and recorded in persistent storage by the Certification Authority, and sends the certificate to the secure application station 30, step 10. It will be understood by those skilled in the art, that instead of the biometric data themselves, a hash of these data may be compared. The biometric data can now be used to authenticate the user on-line.

On the other hand, if it is determined in step 94 that the Session-ID the same or smaller than the last session ID received, forgery or tampering with the Biometric Analyzer Device should be suspected. In this case, the Certification Authority will not issue a certificate and may even disable future use of the device, step 96.

It will be apparent to those skilled in the art that the use of symmetric or asymmetric key arrangements will depend on the security of the respective transmission channel. Over dedicated secure lines, data may be encrypted with a symmetric key, whereas, for example, transmission over the Internet requires asymmetric encryption. Symmetric key encryption is typically significantly faster than asymmetric encryption.

The exemplary authentication process described above may be processed on-line in real time, with signature authentication typically being completed in approximately 1 second. Alternatively, the biometric data may also be used off-line for verification at a later stage.

While the invention has been disclosed in connection with the preferred embodiments shown and described in detail, various modifications and improvements thereon will become readily apparent to those skilled in the art. Accordingly, the spirit and scope of the present invention is to be limited only by the following claims.

We claim:

Claims:

1. A secure transaction system for authenticating a user, comprising:

a biometric analyzer device receiving biometric data of the user and having a secure device identifier;

first authentication means which receive the biometric data and authenticate the biometric data of the user based on biometric reference data of the user; and

second authentication means which authenticate an authorized use of the biometric analyzer device based on at least the secure device identifier,

wherein the secure transaction system authenticates the user if both the first and second authentication means authenticate the biometric data and the authorized use of the biometric input device, respectively.

2. The transaction system according to claim 1, wherein the biometric analyzer device generates a unique session ID for each user session.

3. The transaction system according to claim 2, wherein the unique session ID is sequentially increasing from one session to a following session.

4. The transaction system according to claim 1, wherein the biometric analyzer device further includes a unique biometric analyzer key issued by a trusted device authority.

5. The transaction system according to claim 4, wherein the biometric analyzer device is programmed by a secure programming device having a secure programming station identification key which is known to the trusted device authority.

6. The transaction system according to claim 1, wherein the biometric data received by the first authentication means are in the form of a hashed message digest.

7. The transaction system according to claim 2, wherein the first authentication means compares the current session ID of the biometric analyzer device with the session ID of the previous session and authenticates the user only if the current session ID is greater than the session ID of the previous session.

8. The transaction system according to claim 4, wherein the second authentication means compares the unique biometric analyzer key of the biometric analyzer device with a reference key for the same device.

9. The transaction system according to claim 1, wherein the biometric reference data of the user are stored by a certification authority.

10. The transaction system according to claim 1, wherein the biometric reference data are in the form of a hashed message digest.

11. A method for authenticating biometric data of a user, comprising:

providing a biometric analyzer device with a secure device identifier,

acquiring with the biometric analyzer device biometric data of the user,

generating a sequentially increasing session ID for successive acquisitions of the biometric data,

authenticating the biometric analyzer device based on at least the secure device identifier, and

authenticating the biometric analyzer data based on at least the session ID and a comparison between the acquired biometric analyzer data and reference biometric data for the user,

wherein the biometric data are authenticated only if both the biometric analyzer device and the biometric analyzer data are authentic.

12. The method of claim 11, wherein the comparison between the acquired biometric analyzer data and reference biometric data for the user includes comparing a hash of the respective biometric analyzer data and reference biometric data.

13. The method of claim 11, wherein the secure device identifier is supplied to the biometric input device by a secure programming device.

14. The method of claim 13, wherein the secure programming device comprises a secure programming station identification key.

15. The method of claim 14, wherein the secure programming station identification key is provided to the secure programming device by a trusted device authority.

16. The method of claim 11, wherein authenticating the biometric analyzer device further includes comparing a biometric analyzer key of the biometric analyzer device with a reference key maintained by a trusted device authority.

17. A method for providing end-to-end security in a transaction using biometric data, comprising:

programming a biometric analyzer device with a secure device identifier,

assigning a secure device key to the biometric analyzer device,

acquiring the biometric data with the biometric analyzer device, the biometric analyzer device generating a respective sequentially increasing session ID for successive recordings of the biometric data, and

authenticating the biometric data based on at least the secure device identifier, the device key and the session ID, and on a comparison of a representation of the acquired biometric data with a representation of reference biometric data recorded with the same biometric analyzer device.

18. The method of claim 17, wherein the representation of the biometric data is a hash.

19. The method of claim 17, wherein programming includes connecting said biometric analyzer device to a secure programming device capable of reading a chip identification of the biometric analyzer device, generating a sequence number and obtaining from a device authority a biometric analyzer key pair based on a programming station identification key stored in the secure programming device.

20. The method of claim 19, wherein the private key of the biometric analyzer key pair is embedded in the biometric analyzer device.

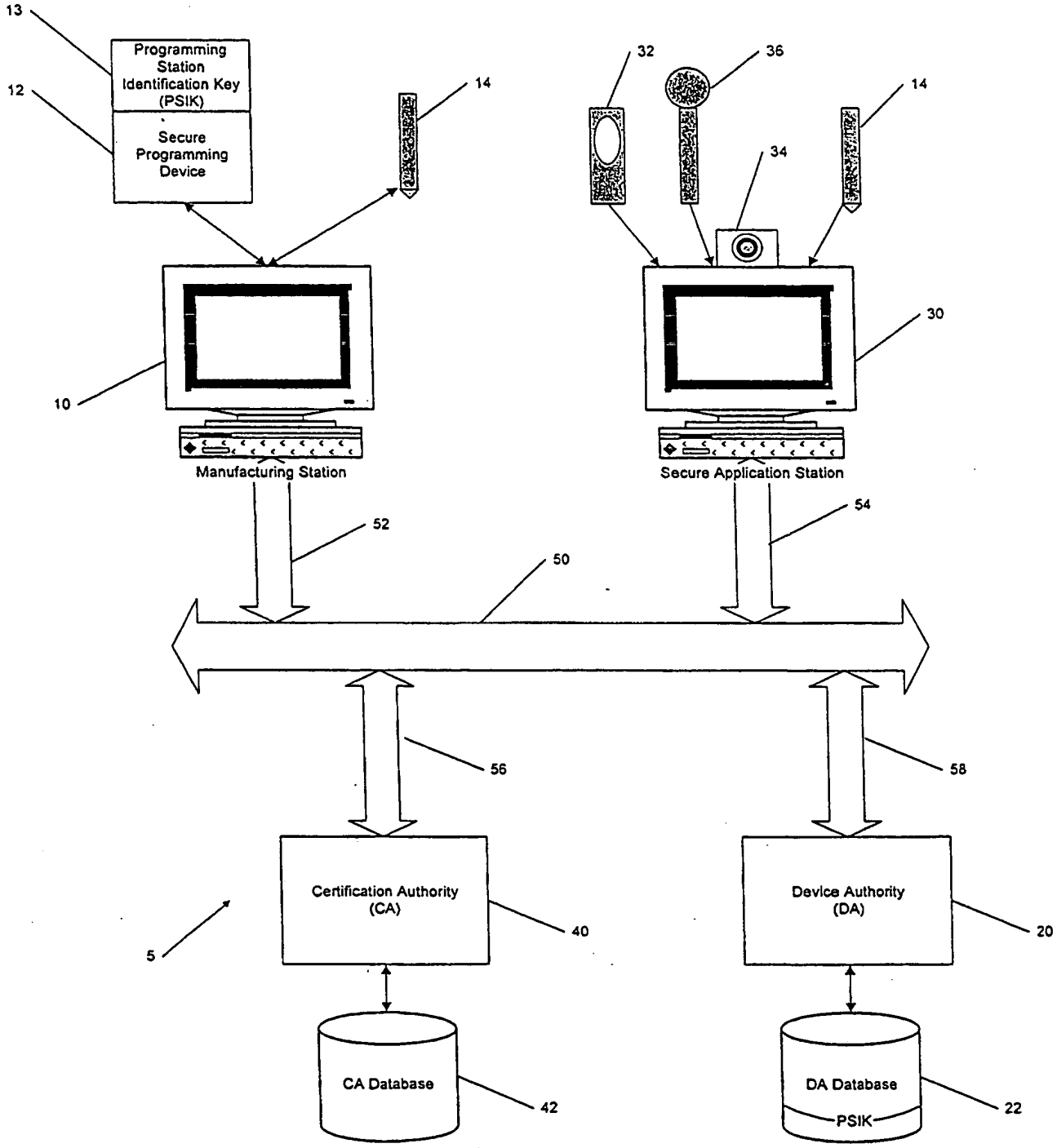

13
Programming Station Identification Key (PSIK)
12
Secure Programming Device
14
32
36
14
34
30
10
Manufacturing Station
Secure Application Station
52
54
50
56
58
Certification Authority (CA)
40
Device Authority (DA)
20
5
CA Database
42
DA Database
PSIK
22

FIG. 1

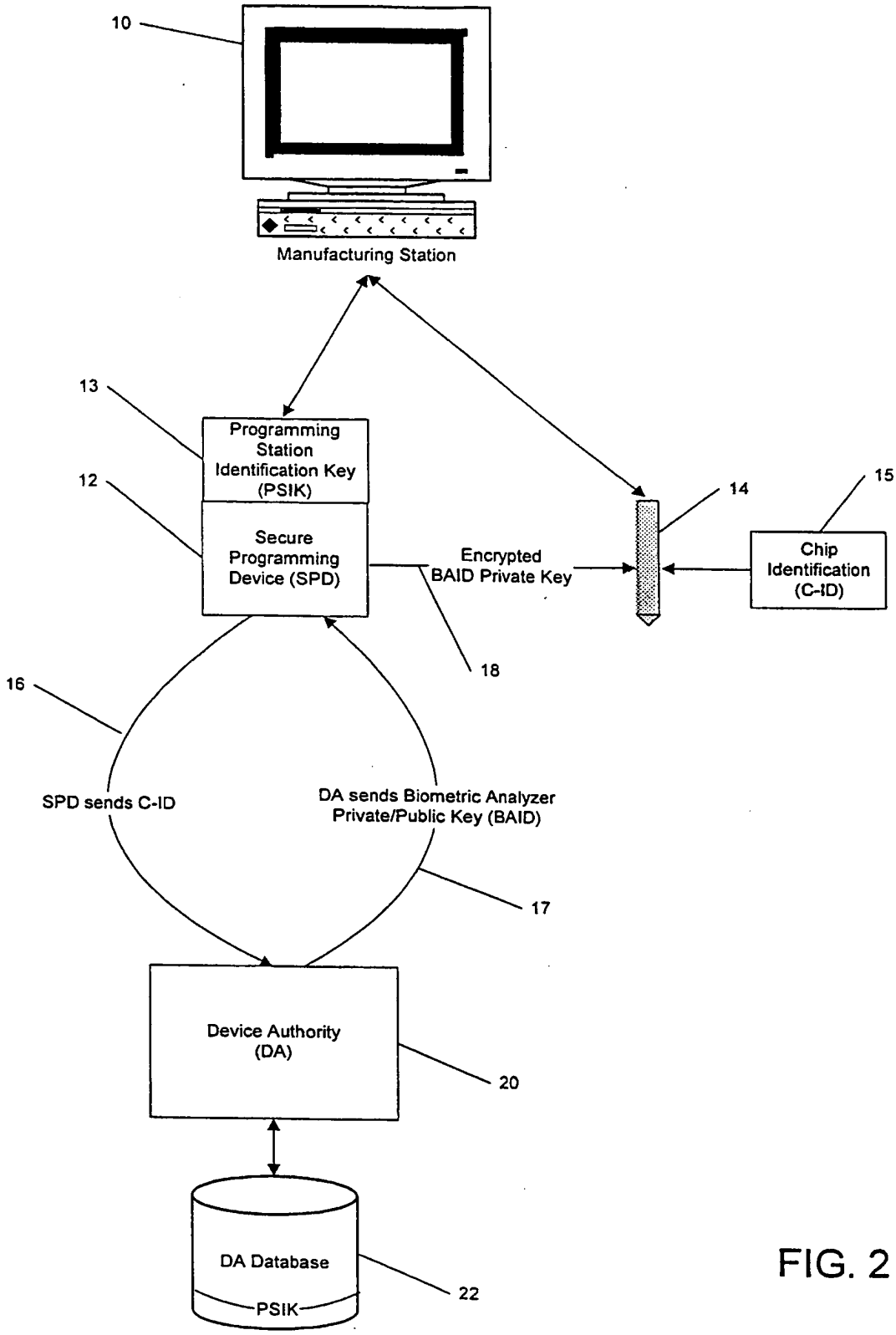

10
Manufacturing Station
13
Programming Station Identification Key (PSIK)
12
Secure Programming Device (SPD)
14
15
Chip Identification (C-ID)
Encrypted BAID Private Key
18
16
SPD sends C-ID
DA sends Biometric Analyzer Private/Public Key (BAID)
17
Device Authority (DA)
20
DA Database
PSIK
22

FIG. 2

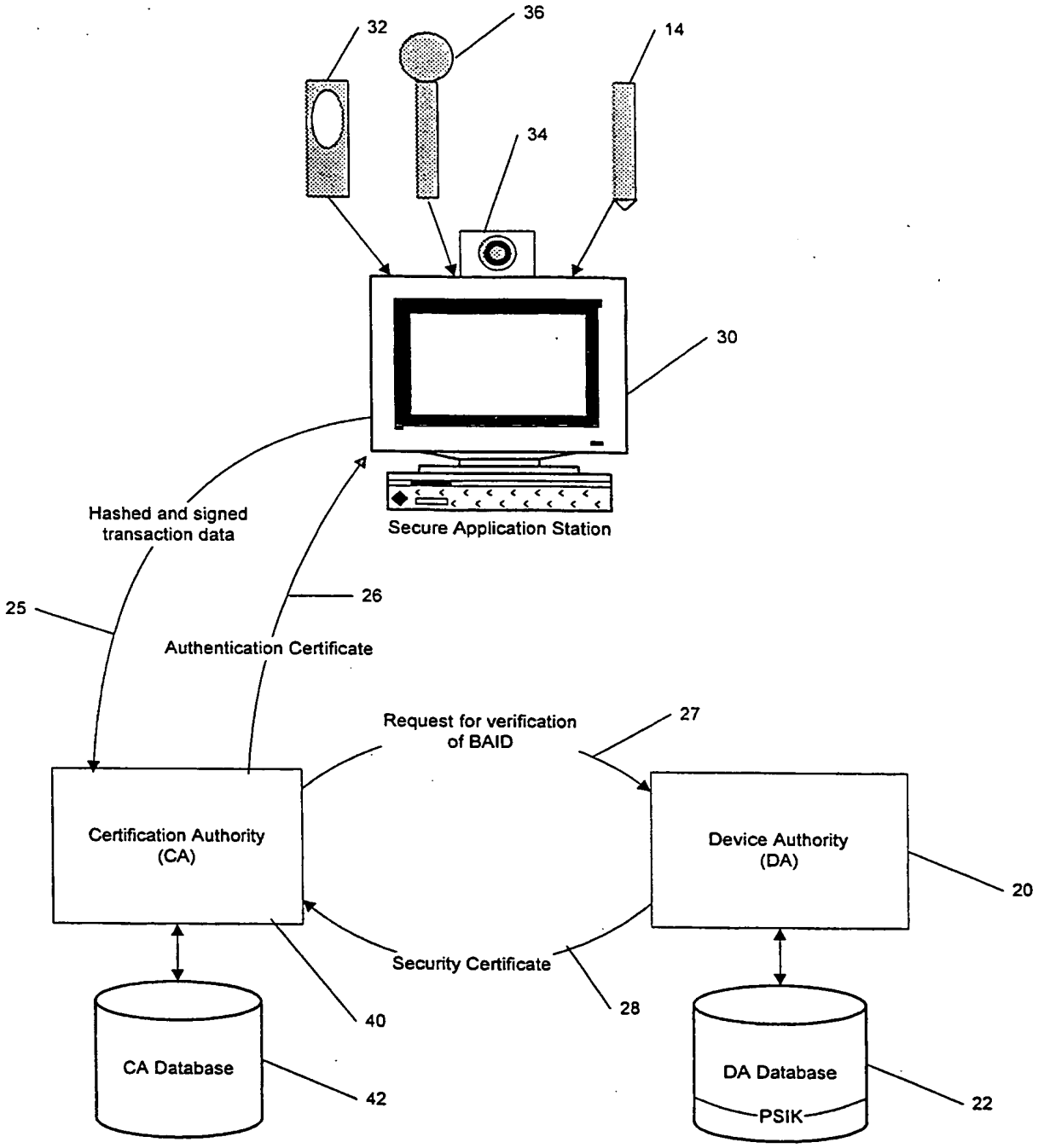

32
36
14
34
30
Secure Application Station
Hashed and signed transaction data
25
26
Authentication Certificate
Request for verification of BAID
27
Certification Authority (CA)
Device Authority (DA)
20
Security Certificate
28
40
CA Database
42
DA Database
PSIK
22

FIG. 3

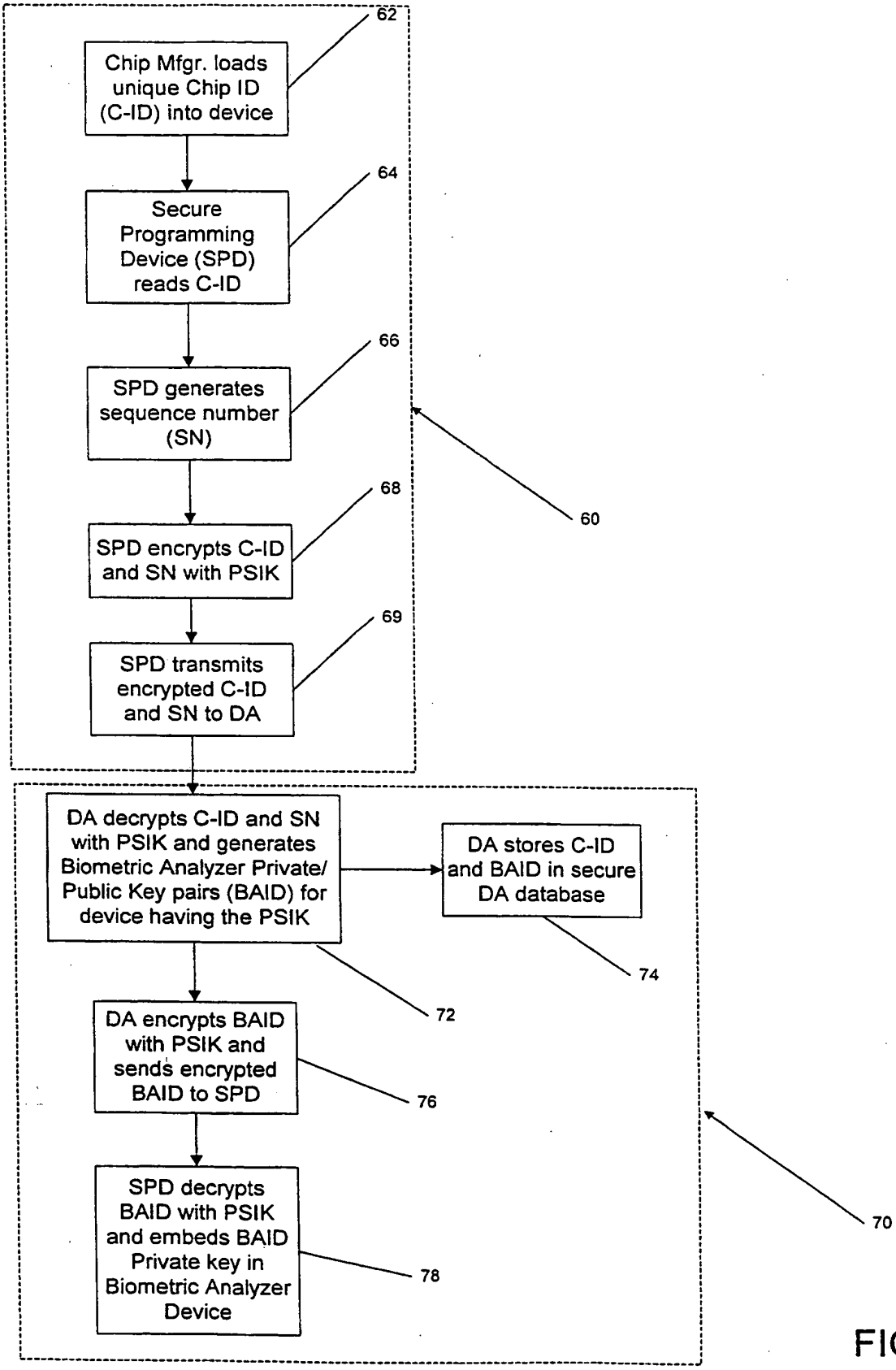


FIG. 4

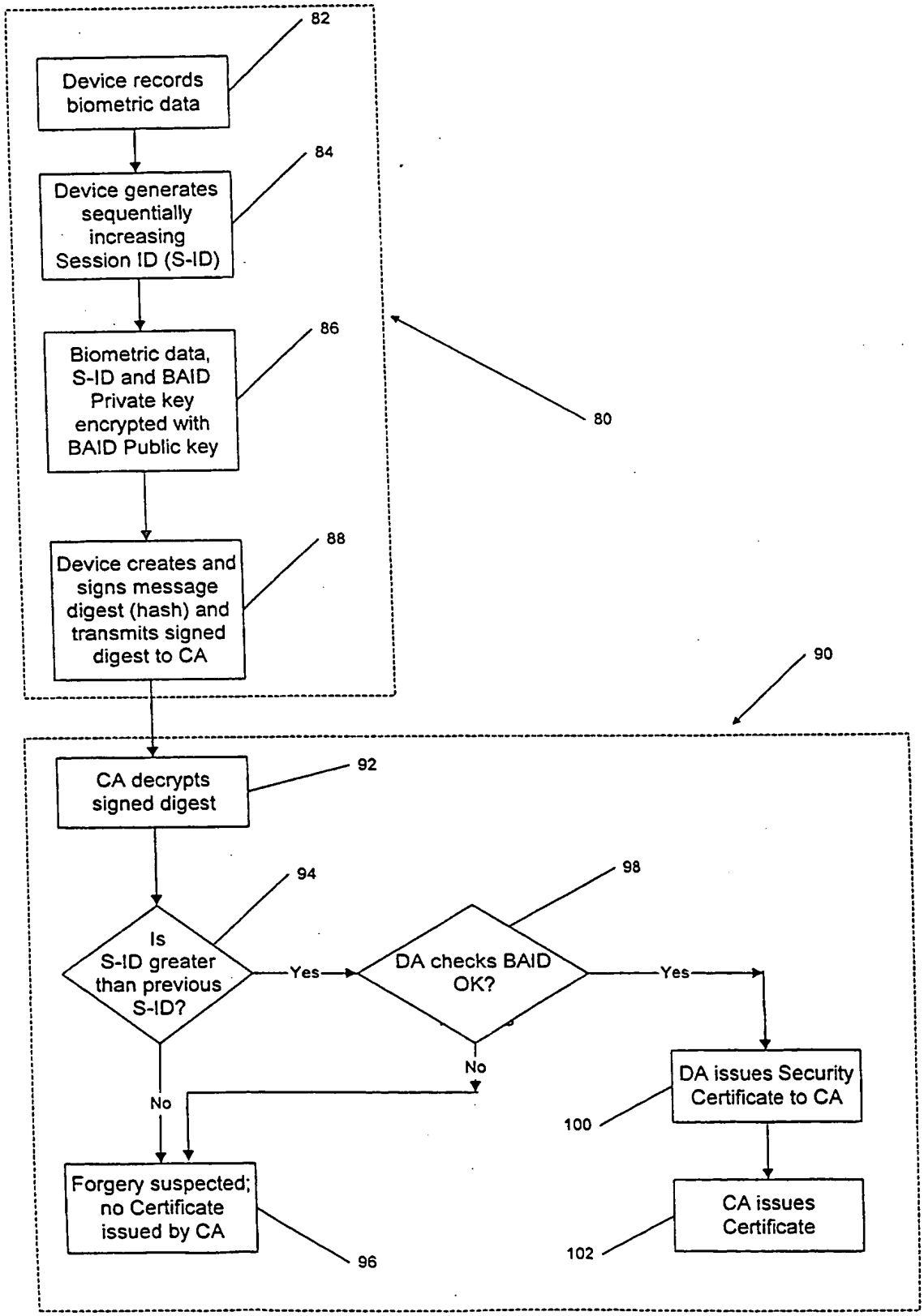


FIG. 5

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **G07F 7/10, G06F 1/00, G07C 9/00**

A3

(11) International Publication Number: **WO 00/00882**

(43) International Publication Date: 6 January 2000 (06.01.00)

(21) International Application Number: PCT/US99/14554

(22) International Filing Date: 25 June 1999 (25.06.99)

(30) Priority Data:
60/090,822 27 June 1998 (27.06.98) US

(71) Applicant: LCI/SMARTPEN, N.V. [US/US]; 952 Beacon Street, Newton, MA 02159 (US).

(72) Inventor: DE SCHRIJVER, Stefaan, A.; 952 Beacon Street, Newton, MA 02159 (US).

(74) Agents: KELLY, Edward, J. et al.; Foley, Hoag & Eliot, LLP, One Post Office Square, Boston, MA 02109 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

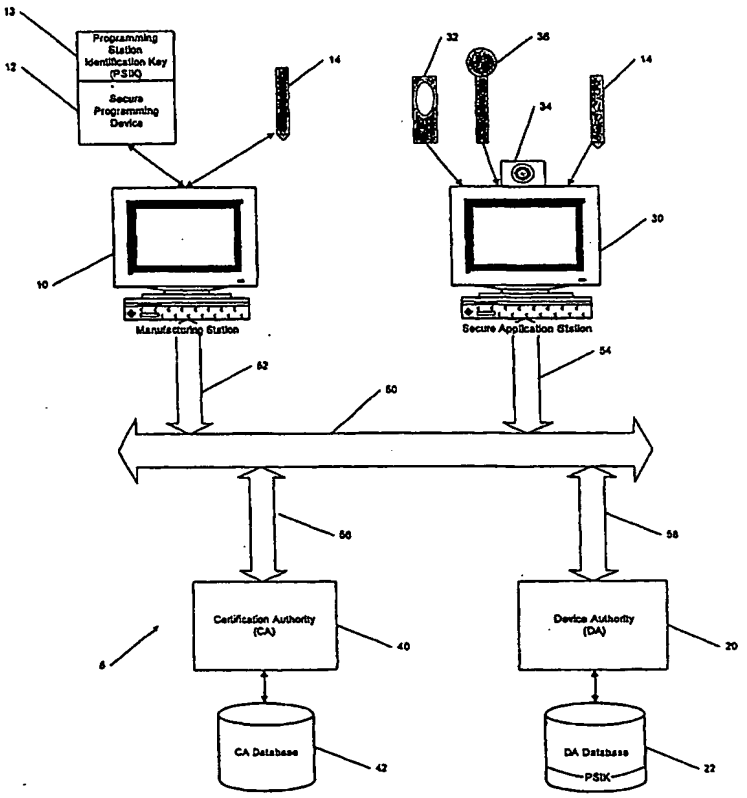
Published
With international search report.

(88) Date of publication of the international search report:
13 April 2000 (13.04.00)

(54) Title: APPARATUS AND METHOD FOR END-TO-END AUTHENTICATION USING BIOMETRIC DATA

(57) Abstract

A secure transaction system and a secure method for authenticating a user based on biometric data of the user includes a biometric analyzer device that is assembled in a secure environment and has a secure device identifier and encryption key. First authentication means receive the biometric data and authenticate the biometric data of the user based on biometric reference data from the user, while second authentication means authenticate an authorized use of the biometric analyzer device based on at least the secure device identifier. The secure transaction system authenticates the user only if both the first and second authentication means authenticate the biometric data and the authorized use of the biometric input device, respectively.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/14554

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 G06F1/00 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F G06F G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 36934 A (SMART TOUCH L L C) 21 November 1996 (1996-11-21) the whole document page 8, line 30 -page 10, line 35 page 20, line 20 -page 6, line 18	1-3,7,9, 11,17, 19,20
Y	page 35, line 1 -page 36, line 10 page 52, line 1 -page 53, line 16 page 80, line 10 -page 81, last line page 123, line 1 -page 127, last line	6,10,12, 18
A		4,5,8, 13-16

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 January 2000	04/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 99/14554

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9636934 A	21-11-1996	US 5613012 A	18-03-1997
		AU 5922696 A	29-11-1996
		BR 9608580 A	05-01-1999
		CA 2221321 A	21-11-1996
		CN 1191027 A	19-08-1998
		EP 0912959 A	06-05-1999
		JP 11511882 T	12-10-1999
		US 5838812 A	17-11-1998
		US 5870723 A	09-02-1999
		US 5764789 A	09-06-1998
		US 5802199 A	01-09-1998
		US 5805719 A	08-09-1998
US 5249230 A	28-09-1993	NONE	
DE 4336679 A	04-05-1995	NONE	